

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:

USA v. 20-41-05

Case No. 5:20-mj-248

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed (*identify the person or describe the property to be seized*):

Evidence of a crime in violation of 18 U.S.C. §§ 1028A, 1956, 1343, 1341, 371, 1349. See Affidavit in Support of Application for Search Warrant, and ATTACHMENT B, which is attached to and incorporated in this Application and Affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

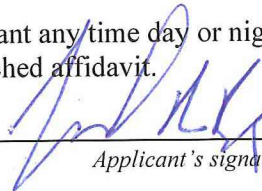
The search is related to a violation of:

Code Section
 18 U.S.C. § 1028A
 18 U.S.C. § 1956
 18 U.S.C. § 1343
 18 U.S.C. § 1341
 18 U.S.C. §§ 371, 1349

Offense Description
 Aggravated Identity Theft
 Money Laundering
 Wire Fraud
 Mail Fraud
 Conspiracy

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

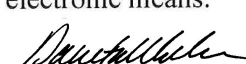

 Applicant's signature

Jared R. Bihr, Special Agent, HSI
 Printed name and title

Sworn to before me and: ☐ signed in my presence.

☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: 12/23/20


 Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
 Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DISTRICT

IN THE MATTER OF THE SEARCH OF:

USA v. 20-41-05

CR 5:20-mj-248

REDACTED
AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION

State of South Dakota)
) ss
County of Pennington)

INTRODUCTION AND AGENT BACKGROUND

I, Jared R. Bihr, Special Agent with Homeland Security Investigations (HSI), and currently assigned to HSI Rapid City, South Dakota, being duly sworn, states as follows:

1. I have been a Special Agent (SA) with HSI and with one of the predecessor agencies of HSI, the Immigration & Naturalization Service, since July 1998. Prior to that I was a U.S. Border Patrol Agent for two years. I have statutory authority and I have received specialized training to investigate criminal and administrative violations of the immigration, customs and other criminal laws of the United States. I have successfully conducted criminal investigations pertaining to violations of Titles 8, 18 and 21 of the United States Code and I have submitted affidavits for criminal complaints and search, seizure and arrest warrants. I have also testified in judicial proceedings.
2. During my law enforcement career, I have been involved in the

investigation of cases involving aggravated identity theft, money laundering, wire fraud, mail fraud and conspiracies to commit these offenses in violation of 18 U.S.C. §§ 1028A, 1956, 1343, 1341, and 371/1349, respectively. I have become familiar with the modus operandi of persons involved in the theft and sale of stolen identities to be used for various illegal fraud schemes using electronic communications and the U.S. Postal Service to help facilitate the schemes. Based on my training and experience, I am also familiar with various methods of laundering money and transferring illicit proceeds generated from such fraudulent schemes.

3. I am aware that 18 U.S.C. §§ 1028A, 1956, 1343, 1341 and 371/1349 prohibit the unlawful use of another person's identity in relation to certain felonies, the laundering of illicit proceeds generated from such unlawful activity, the use of electronic communications or the U.S. Postal Service to help facilitate these unlawful activities and conspiracies to commit these offenses.
4. The facts set forth in this affidavit are based on my personal knowledge; knowledge obtained from other individuals, including other law enforcement officers; interviews of persons with knowledge; my review of documents, interview reports and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. This affidavit contains

information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, no information known to me that would tend to negate probable cause has been withheld from this affidavit.

ITEMS TO BE SEARCHED FOR AND SEIZED

5. This affidavit is submitted in support of an application for a search warrant for the contents of and information pertaining to a TextNow Inc. account found during the investigation of an unknown subject utilizing the TARGET ACCOUNT, which is more specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 1028A, 1956, 1343, 1341, and 371/1349 (aggravated identity theft, money laundering, wire fraud, mail fraud and conspiracy), and which items are more specifically described in Attachment B. The specific TextNow Inc. telephone number is: **619-720-0732** (also referred to in this affidavit as "Target Account").

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachments A and B:
 - a. "Chat," as used herein, refers to any kind of text communication transmitted over the Internet in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format, that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

- b. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that individuals can use to store and trade information in larger volumes. Users of such a service can share links and associated passwords to their stored files with other individuals in order to grant access to their information. Such services allow individuals to access these files easily through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.
- c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).
- d. "Computer hardware," as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives,

floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- e. "Computer software," as used herein, is digital information, which a computer can interpret and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- f. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or passphrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include

programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- h. A provider of “Electronic Communication Service” (“ESP”), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.
- i. “Electronic Storage Device” includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.
- j. “File Transfer Protocol” (“FTP”), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.
- k. “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer to access the Internet. IP addresses

can be “dynamic,” meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

- l. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.
- m. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.
- n. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- o. “Short Message Service” (“SMS”), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows the user to send short text messages from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical,

electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

- p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON AGGRAVATED IDENTITY THEFT, MONEY LAUNDERING, WIRE FRAUD, MAIL FRAUD, COMPUTERS, THE INTERNET, AND EMAIL

7. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interact with each other. Computers serve many functions for persons who are involved with the theft and sale of personal identifying information to be unlawfully used in fraudulent schemes designed to generate illicit proceeds; they serve as a mechanism for stealing personal identifying information or to purchase stolen identifying information; they serve as a mechanism to use the stolen identifying information in furtherance of sophisticated fraudulent schemes.

b. Persons who trade in stolen identities to be used for fraudulent

schemes for financial gain can transfer printed identification documents into a computer-readable format with a device known as a scanner and then distribute the images using email or messaging services like TextNow Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to trade in stolen identifying information easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of theft

and distribution of stolen identifying information. Persons can transfer stolen identifying information and related information used to facilitate fraud schemes via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "instant messaging"), and easy access to the Internet, the computer is a preferred method of trading stolen identifying information among co-conspirators involved in aggravated identify theft, money laundering, wire fraud and mail fraud.

8. Based on my training and experience and investigation in this case, I have learned the following about TextNow Inc.:
 - a. TextNow is an electronic communications service accepting service of process at Attn: Registered Agent of Process for TextNow Inc., GKL Corporate/Search, Inc., Capitol Mall, Suite 660, Sacramento, CA 95814. TextNow Inc. (no comma) is the United States-based location for TextNow, Inc. (with comma) at 420 Wes Graham Way, 2nd Floor, Waterloo, Ontario, Zip Code N2L 0J6, Canada (the Provider), as described in Attachment A to the proposed warrant.
 - b. TextNow is a voice over Internet Protocol (VoIP) service that allows its users to text and call any number in Canada and the United States. TextNow provides users with a real phone number which can be used on any smartphone, tablet, or desktop computer with an internet connection. The application can be used on multiple devices under

the same login at the same time.

- c. TextNow collects subscriber data from their customers including customer's username, phone number, name, email address, date of birth, phone ownership from date, phone ownership to date, and the registration IP address used by the customer. Subscriber data lists the basic account information related to either the provided username or phone number. If a phone number is provided, all the usernames associated to the phone number within the requested timeframe will be provided. If a username is provided, all phone numbers associated to the account within the requested timeframe will be provided.

Phone numbers may be recycled from dormant users. This means that a phone number identifier may be assigned and reassigned to different users at different times.
- d. TextNow maintains message logs from their customers. Message logs are a transactional record outlining when a TextNow user sent or received a text message. They include the date and time the transaction occurred, the direction of the transaction, the contact phone number, and indicate whether the user has deleted the message.
- e. TextNow also retains the content of the text messages. The content of the messages may include media that was sent or received or the transcript of the message.
- f. TextNow retains call logs involving their customers. Call logs are a

transactional record outlining when a TextNow user made or received a call. They include the call start date and time, the caller and called number, as well as the duration of the call listed in seconds. TextNow also retains the content of voicemails.

- g. TextNow also retains internet protocol (IP) logs involving their customers. IP logs contain the IP address and its corresponding timestamp.
- h. TextNow also retains media sent or received by their customers. Media may include images, videos, or voicemails sent or received by TextNow users. Each media file will have a unique identifier that will also be listed in the message logs to indicate when each piece of media was sent or received.
- i. In summary, based on my training and experience, there is probable cause to believe that the computers of TextNow are likely to contain user-generated content such as stored electronic communications, as well as TextNow-generated information about its subscribers and their use of TextNow services and other related services. In my training and experience, all that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide TextNow with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities. Information stored in connection with a TextNow account

may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a TextNow account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, text messaging communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by TextNow can show how and when the account was accessed or used. For example, providers such as TextNow typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the TextNow account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a time (e.g., location information

integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the TextNow account may indicate its user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

9. From my training and experience, I am aware that TextNow's computers contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer accounts and/or files for information and the content of communications pertaining to the Target Account specified herein and in Attachment A, following the procedures described herein.

PROBABLE CAUSE

10. In October 2020 HSI Rapid City initiated a financial fraud and money laundering investigation based on information received from the United States Air Force (USAF) Office of Special Investigations (OSI) at Ellsworth Air Force Base, South Dakota. On 09/18/2020, USAF OSI Special Agent Benjamin Enterline interviewed an individual, who will be hereinafter referenced as Subject 1, regarding a job Subject 1's spouse (referenced as Subject 2), had obtained via the employment website "Indeed." Based on the type of tasks Subject 2 was being asked to

perform, Subject 1 and Subject 2 became suspicious that the job Subject 2 obtained was not legitimate.

11. Special Agent Enterline took a written statement from Subject 1, obtained copies of Subject 2's text messages between Subject 2 and the employer of concern, ("Ray White") and screenshots of Subject 2's USAA cellular telephone banking application which show multiple deposits into Subject 2's account from "New York State (unemployment) Paycheck." Special Agent Enterline then referred the information to HSI Rapid City Special Agent Jared Bihr.
12. According to the text messages between Subject 2 and his/her employer "Ray White" which began on 07/23/2020, part of the job requirements was to "buy gifts and send money to families and children's homes." Subject 2 was to work remotely approximately five to nine hours per week and would be paid US\$700.00 weekly.
13. Some verbatim excerpts from the text conversations between "Ray White" and Subject 2 are included above and below. Not all the text messages are included in this affidavit, but they are included in the case file for this investigation. The Target Account has been highlighted with bold text.
14. "Ray White" was to have the money for salary and purchases deposited directly into Subject 2's bank account. Subject 2 sent his/her ACH banking information to the email address:
raywhitecement795@gmail.com.

15. Subject 2 and "Ray White" continued to communicate via text messages. On or about 08/26/2020, several weeks after sending his/her ACH banking information, Subject 2 began receiving multiple payments into his/her banking account. The deposits initially totaled approximately US\$13,240.00. On 08/27/2020 "Ray White" messaged Subject 2: "Hi (Subject 2), please confirm if you received a deposit." Subject 2 replied: "I did, I am traveling back to South Dakota today so I will be in an (sic) out of service with my phone on the plane, but I received several transactions for \$600 and \$182. If you need me to call when I am back in an airport to figure out anything I can." "Ray White" replied: "How much is the total deposit? when will you be available to carry out the tasks? travel safe." Subject 2 replied: "The total all together was \$13,240. I get home at 5pm mountain time today and I am available to start right away." With some of the money, "Ray White" instructed Subject 2 to: "please buy four units of \$1000 USPS Money order, please make them blank ones, Don't make them payable to anyone." "Ray White" then instructed Subject 2 to have the United States Postal Service (USPS) money orders sent overnight to: "PJ Logistics, [REDACTED], Houston, Texas 77083." "Ray White" also instructed Subject 2 to: "please deduct \$600 for your wages."

16. A few days later, on 08/31/2020, "Ray White" instructed Subject 2 to send another US\$4,000.00 in USPS money orders to PJ logistics. One day after that on 09/01/2020, "Ray White" instructed Subject 2 to send

another US\$4,000.00 to: "A & S Agency, [REDACTED],
Philadelphia, PA 19153."

17. On 09/02/2020, "Ray White" asked Subject 2 "Can you please sign up for bitcoin.com." "Ray White" walked Subject 2 through the steps of downloading the bitcoin application to Subject 2's cellular telephone and then asked her to: "Please buy \$900 BTC 1HPRZaaqxr3oJuyAu4RkaX5u9xctdyrH1Y." Subject 2 replied to "Ray White:" "Out of the \$13,240 sent to me I have spent \$12,700 from the money orders and my wages, so I only have \$540 left of what was deposited into my account." "Ray White" replied: "oh.. I am sorry I didn't do the calculation try to send \$400." Later on 09/02/2020, Subject 2 sent the following message to "Ray White:" "Everything has been approved and sent to 1HPRZaaqxr3oJuyAu4RkaX5u9xctdyrH1Y." "Ray White" replied: "Sure. Let me tell the recipient to check."
18. Later, on 09/02/2020, "Ray White" messaged Subject 2: "You will receive another transfer next week. Can you please open an account at another financial institution." Subject 2 replied: "Absolutely. I can do that tomorrow and send you the new information right away."
19. "Ray White" and Subject 2 continued to message about Subject 2 opening a bank account. The following messages are verbatim excerpts of the remaining text messages between "Ray White" and Subject 2.
- a. "Ray White:" "Sure. I would appreciate that. Which financial institution?"

- b. Subject 2: "There's two larger banks around me. My options would be US bank or First Interstate Bank."
 - c. "Ray White:" "Open both if you can."
 - d. Subject 2: "Open one checking account at both accounts, correct?"
 - e. "Ray White:" "yes. Do send me the info as soon as possible and tell them you'll be handling 20K in each account monthly."
 - f. Subject 2: "Will do. Will I still be using the current bank I have sent you or just the two new ones?"
 - g. "Ray White:" "all of them." AND: "To avoid transfer delays" AND: "the last transfer took quite a while before it hit your account."
 - h. Subject 2: "Got it. Should I use some of the money in my current account to open the new ones or my personal money? I'm not sure how much I will have to put in to open it."
 - i. "Ray White:" "use the money left to open the new account. No need to use your money :-)"
 - j. Subject 2: "Perfect. Thank you!"
20. On 09/03/2020, the text message conversation between "Ray White" and Subject 2 continued:
- a. Subject 2: "The inside of our banks are closed due to Covid, so I called to open an account today and told them the situation in handling 20K in the account monthly and basically they told me that if I don't have any legal documentation to handle your money they look at it as money laundering and won't allow me to open the account. I'm not

sure how to go about opening the account, or I don't have the correct information to give them to open it."

- b. "Ray White:" "Do you have a savings account with your current institution?"
- c. Subject 2: "yes."
- d. "Ray White:" "Is that the account number you provided?"
- e. Subject 2: "the account number you have is my checking account."
- f. "Ray White:" "Oh. Let's try your savings."
- g. Subject 2: "I am just wondering why the bank suspected me of money laundering, I need to know that what I'm doing isn't illegal for my family. The way the bank spoke to me, it seemed like if something happened I would be the one to get into trouble for this."
- h. "Ray White:" "Far from it (Subject 2). Banks do these checks all the time to avoid money laundering especially during covid-19" AND:
"There is nothing to worry about" AND: "You can walk into any bank and open an account if you want. I had to tell you to tell them because sometimes banks hold deposits for further verification." AND:
"I only wanted to avoid that in your case."
- i. Subject 2: "I understand, I just want to make sure I'm not doing something to put myself or my family into trouble. Is there any documentation to show that I am working for your company and using your money for tasks that you need completed. I would also be okay with paper checks mailed to me that I can personally put into

my account if that would work for you."

- j. "Ray White:" "Sure. I will see what I can do - - there's actually nothing to be worried about"

21. 09/04/2020 text messages between "Ray White" and Subject 2:

- a. "Ray White:" "Hi (Subject 2), how are you today?"
- b. Subject 2: "I'm doing good, how are you?"
- c. "Ray White:" "I am doing well. I have initiated another transfer."
- d. Subject 2: "Great, I will keep my eye out for it. I have also been looking for the paperwork and tax forms being mailed but I haven't seen anything. Should I be expecting them soon?"
- e. "Ray White:" "Yes. I will get them out as soon as I can. Sorry for the delay"
- f. Subject 2: "No worries, just making sure I haven't missed anything since I was out of town for a while."

22. 09/09/2020 text messages between "Ray White" and Subject 2:

- a. "Ray White:" "Hi (Subject 2), how are you doing?" (Subject 2 did not reply)"Ray White:" "Hi (Subject 2) are you getting my messages?"

23. Subject 2's bank account received five additional US\$300.00 deposits and one additional US\$182.00 deposit from the New York State unemployment office from about 09/10/2020 through about 09/24/2020.

TELEPHONIC INTERVIEW OF SUBJECT 2:

24. On 10/22/2020, HSI Rapid City Special Agent Jared Bihr

interviewed Subject 2 telephonically via his/her cellular telephone. After being advised of Special Agent Bihr's identity and the nature of the interview, Subject 2 provided the following information:

25. Subject 2 was looking for a job working remotely and was using the employment website "Indeed" to look for jobs. He/she applied to a job announcement for a customer service representative for "Ray White Cement Company." The job is still posted on "Indeed" but is listed as "expired." "Ray White Cement Company" also has a "Facebook Page."

26. Later on 10/22/2020, Subject 2 provided telephonic consent to access his/her "Indeed" account. The provided consent was witnessed over a speaker telephone with HSI Rapid City Criminal Analyst Amber Cooper as a second witness. Criminal Analyst Cooper accessed Subject 2's "Indeed" account while Subject 2 was still on the telephone and took computer screen shots of the job posting and correspondence on "Indeed." The URL for the "Indeed" posting was:
https://www.indeed.com/viewjob?from=app-tracker-post_apply-appcard&hl=en&jk=3d06375b3e8a9ee7&tk=1e19378mcu431800. Screen shots of the "Ray White Cement Company Facebook Page" were also taken.

27. **After applying for the job on "Indeed" Subject 2 was contacted via text message from telephone number: 619-720-0732 by "Ray White."** "Ray White" got Subject 2's telephone number via "Indeed" and offered her the job. Their communications are saved in her text

messages. Subject 2 received the money from "Ray White" to his/her USAA checking account. The routing number for his/her account is: [REDACTED] 4269 and his/her account number is: [REDACTED] 7589.

28. Since all of this happened, USAA has frozen Subject 2's checking account. USAA told her that the account would still be able to receive deposits but withdrawals would not be allowed. USAA customer service told Subject 2 the account would be frozen until 11/16/2020.

29. Subject 2 is still in possession of the receipts for all the USPS money orders she mailed as directed by "Ray White." The receipts include the individual serial numbers for each money order. All the money orders he/she purchased and mailed were valued at US\$1000.00 and had the payer and payee portions of the money orders left blank. He/she was directed to leave the money orders blank by "Ray White" and "Ray White" also told him/her where to send them.

30. USPS Money Orders sent overnight to PJ Logistics, [REDACTED], Houston, TX 77083 on 08/28/2020: USPS Tracking Number: EJ443093249US; USPS Money Order Serial Numbers: 26619184113; 26619184124; 26619184135; 26619184146.

31. USPS Money Orders sent overnight to PJ Logistics, [REDACTED], Houston, TX 77083 on 08/31/2020: USPS Tracking Number: EJ362773326US; USPS Money Order Serial Numbers: 26619184260; 26619184271; 26619184282; 26619184293.

32. USPS Money Orders sent to A & S Agency, [REDACTED],

Philadelphia, PA 19153: USPS Tracking Number: EJ035587391; USPS Money Order Serial Numbers: 26565849876; 26565849887; 26565849898; 26565849900.

33. Subject 2 sent photographs of the USPS money orders to Special Agent Bihr via email.

INFORMATION OBTAINED FROM USPS PERTAINING TO THE USPS MONEY ORDERS:

34. Special Agent Bihr contacted USPS Postal Inspector Rapid City Brent Brandner regarding the above referenced USPS money orders. Postal Inspector Brandner obtained images of all the cashed money orders.
35. The four US\$1000.00 USPS Money Orders sent overnight to PJ Logistics, [REDACTED], Houston, TX 77083 on 08/28/2020 were all made "Pay to;" Obayomi KADIRI (address blank) and were made "From:" Sheriff Adigun, [REDACTED], Houston, TX 77082. The Bank of First Deposit (BOFD) for these money orders is: First National Bank of Texas (routing number: [REDACTED] 6271). They were negotiated on 08/31/2020. The subsequent bank is: Wells Fargo (routing number: [REDACTED] 0019). The negotiation date for the subsequent bank is 09/01/2020.
36. The four US\$1000.00 USPS money orders sent to PJ Logistics, [REDACTED], Houston, TX 77083 on 08/31/2020 were all made "Pay to;" Shakirat KADIRI (address blank) and were made "From:" Sheriff

Adigun, [REDACTED], Houston, TX 77082. The BOFD for these money orders is: Wells Fargo (routing number: [REDACTED]0019). They were negotiated on 09/01/2020.

37. The four US\$1000.00 USPS money orders sent to A & S Agency, [REDACTED], Philadelphia, PA 19153 were all made "Pay to:" Aminat SULIAMAN, [REDACTED] and were made "From:" Aminat SULIAMAN, [REDACTED]. The BOFD for these money orders is: Bank of America (routing number: [REDACTED]0138). Two of these money orders were negotiated on 09/08/2020, one on 09/16/2020, and one on 09/25/2020.

38. Open-source, commercial record checks for address [REDACTED], [REDACTED], Houston, TX 77083 revealed this address pertains to an owner-occupied single-family residence. The owner listed for this property is Shakirat KADIRI and the co-owner listed is Obayomi KADIRI. Open-source, commercial record checks for address [REDACTED], Philadelphia, PA 19153 revealed this address pertains to an apartment complex. One of the residents listed at this apartment complex is Aminat SULIAMAN.

INFORMATION OBTAINED FROM NEW YORK STATE DEPARTMENT OF
LABOR OFFICE OF SPECIAL INVESTIGATIONS:

39. On 10/30/2020, Special Agent Bihr spoke with New York State Department of Labor, Office of Special Investigations, Major Case Unit, Chief Investigator Michelle Martone. Investigator Martone explained that

the New York State Department of Labor is experiencing an enormous, unprecedented number of cases of suspected fraud due to the COVID-19 pandemic and the associated payments her agency is responsible for handling.

40. Investigator Martone checked for any New York Department of Labor unemployment insurance payments made to routing number: [REDACTED] 4269 and account number: [REDACTED] 7589 (Subject 2's above referenced bank account). Investigator Martone found one unemployment insurance claim that was in the name of an individual who will be referenced as Victim 1.
41. Over the course of several days, Investigator Martone provided Special Agent Bihr with a copy of the online unemployment insurance application, the Internet Protocol (IP) Address Log connected to this claim, and a spreadsheet containing the unemployment insurance payments made to this account. As of 10/30/2020, the IP addresses used in connection with this claim are:
- a. 69.206.62.1 on 2020-09-09 17:10:21:233 (Eastern Time, ET),
Ulster Park, NY;
 - b. 69.206.62.1 on 2020-09-09 17:09:13:107 ET, Ulster Park, NY;
 - c. 107.77.223.235 on 2020-08-27 13:24:19:656 ET, Philadelphia, PA;
 - d. 47.20.251.79 on 2020-08-26 10:20:07:647 ET, Central Islip, NY;
 - e. 24.191.4.78 on 2020-08-24 13:00:58:399 ET, Bronx, NY;
 - f. 24.191.4.78 on 2020-08-24 12:29:41:18 ET, Bronx, NY;

- g. 24.191.4.78 on 2020-08-24 12:01:29:904 ET, Bronx, NY;
 - h. 24.191.4.78 on 2020-08-24 12:00:29:170 ET, Bronx, NY;
 - i. 104.140.53.75 on 2020-08-19 12:34:50:116, New York City, NY.
42. Investigator Martone also found one telephone number that was connected to this claim and was used to call the New York Department of Labor on 08/20/2020: 630-427-8210.
43. Investigator Martone explained that there are basically three types of payments for this claim her agency is handling. Pandemic Emergency Unemployment Assistance payments can be made to individuals even if they do not have any wages reported to the New York State Department of Labor. Those payments are usually US\$182.00 per week unless the individual can show a history of a high level of wages, in which case the amount of the weekly payments may be increased. Federal Pandemic Unemployment Insurance payments were a temporary payment made for individuals who suffered job losses due to the COVID-19 pandemic. Those payments are usually US\$600.00 per week. Finally, there is also some availability of payments from the Federal Emergency Management Agency. Those payments are usually US\$300.00.
44. Investigator Martone did not find any claims connected to telephone number: **619-720-0732** (the telephone number used to message Subject 2's cellular telephone).
45. The following are the payments that were made by the New York State Department of Labor via direct deposit into Subject 2's bank

account via direct deposit:

- a. Week: 04/12 Amount: \$182.00
- b. Week: 04/12 Amount: \$600.00
- c. Week: 04/19 Amount: \$182.00
- d. Week: 04/19 Amount: \$600.00
- e. Week: 04/26 Amount: \$182.00
- f. Week: 04/26 Amount: \$600.00
- g. Week: 05/03 Amount: \$182.00
- h. Week: 05/03 Amount: \$600.00
- i. Week: 05/10 Amount: \$182.00
- j. Week: 05/10 Amount: \$600.00
- k. Week: 05/17 Amount: \$182.00
- l. Week: 05/17 Amount: \$600.00
- m. Week: 05/24 Amount: \$182.00
- n. Week: 05/24 Amount: \$600.00
- o. Week: 05/31 Amount: \$182.00
- p. Week: 05/31 Amount: \$600.00
- q. Week: 06/07 Amount: \$182.00
- r. Week: 06/07 Amount: \$600.00
- s. Week: 06/14 Amount: \$182.00
- t. Week: 06/14 Amount: \$600.00
- u. Week: 06/21 Amount: \$182.00
- v. Week: 06/21 Amount: \$600.00

w. Week: 06/28 Amount: \$182.00

x. Week: 06/28 Amount: \$600.00

y. Week: 07/05 Amount: \$182.00

z. Week: 07/05 Amount: \$600.00

aa. Week: 07/12 Amount: \$182.00

bb. Week: 07/12 Amount: \$600.00

cc. Week: 07/19 Amount: \$182.00

dd. Week: 07/19 Amount: \$600.00

ee. Week: 07/26 Amount: \$182.00

ff. Week: 07/26 Amount: \$600.00

gg. Week: 08/02 Amount: \$182.00

hh. Week: 08/09 Amount: \$182.00

ii. Week: 08/16 Amount: \$182.00

jj. Week: 08/23 Amount: \$182.00

kk. Week: 09/06 Amount: \$182.00

ll. Week: 08/02 Amount: \$300.00

mm. Week: 08/09 Amount: \$300.00

nn. Week: 08/16 Amount: \$300.00

oo. Week: 08/23 Amount: \$300.00

pp. Week: 09/06 Amount: \$300.00

46. In summary, a total of US\$14,922.00 was deposited into Subject

2's USAA bank account that was intended to be COVID-19 related

benefits that were applied for via the internet using the identity of Victim

1.

TELEPHONIC INTERVIEW OF VICTIM 1:

47. On 11/02/2020, HSI Rapid City Special Agent Jared Bihr interview Victim 1 via his/her cellular telephone. After being of advised of Special Agent Bihr's identity and the nature of the interview, Victim 1 provided the following information:

48. Victim 1 is a retired school principal. Victim 1 possibly had his/her identity stolen about one month previously. He/she received unsolicited bank cards in the mail for a bank account at a bank in Florida that he/she did not open. Victim 1 reported the incident but could not remember all the exact details off-hand. He/she will find the paperwork related to this incident. Victim 1 believes someone opened a bank account using his/her identity to use for some type of fraud scheme.

49. Victim 1 has lived in Nevada for about 26 years. Prior to living in Nevada Victim 1 lived in Arizona for about 13 years. Victim 1 has never been to New York state and has never applied for unemployment benefits in New York state. Victim 1 is willing to meet with an HSI investigator regarding this matter and is available to be contacted again telephonically anytime.

50. Open-source, commercial record checks indicate Victim 1 does reside in Nevada.

51. Special Agent Bihr subsequently found a report filed with the

Federal Trade Commission on or about 08/19/2020 by Victim 1 pertaining to his/her spouse and Victim 1 receiving "GoBank" bank debit cards in the mail for a bank account they did not open.

PRESERVATION REQUEST: TEXTNOW / INTELIGENT, INC.

52. On 10/22/2020, Special Agent Bihr requested HSI Analyst Amber Cooper issue a preservation request for the telephone number: **619-720-0732**. Based on open-source, commercial record checks indicating this telephone number belonged to Inteligent, Inc., Analyst Cooper issued a preservation request to that company.

53. On 10/23/2020, Inteligent, Inc. sent an email to Analyst Cooper indicating telephone number: **619-720-0732** has been assigned to TextNow, Inc. Analyst Cooper issued a preservation request to TextNow, Inc. that same day.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

54. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require TextNow, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A and Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

55. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a “district court of the United States (including a magistrate judge of such court)” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

REQUEST/JUSTIFICATION FOR ORDER OF NONDISCLOSURE

56. The United States respectfully applies for an order of nondisclosure to TextNow Inc. under 18 U.S.C. § 2705(b) regarding the following account: **619-720-0732**. The United States is seeking this search warrant for subscriber information, including all names, addresses, IP addresses, including historical, telephone numbers, other email addresses, information on length and types of services and any means of payment related to these accounts under the authority given by 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Based on § 2703(c)(3), the United States is not required to provide notice to the subscriber. Under § 2705(b), the United States may apply to the court for an order commanding TextNow, Inc. not to notify the subscriber of the existence of the search warrant. The court may decide what length of time shall apply to the order of nondisclosure if the court determines the notification to the subscriber could result in one of the five factors listed in the statute, which includes destruction of or tampering with evidence.

18 U.S.C. § 2705(b)(3). The basis for the request is that such disclosure could cause any person with access to the accounts, or any related account or account information, to tamper with or modify the content or account information and thereby destroy or tamper with evidence and otherwise seriously jeopardize the investigation. Especially due to the ease of access to TextNow, Inc., persons can modify its content with internet access and enough account information. As such, the United States respectfully requests this Court enter an order commanding TextNow Inc. not to notify the user of the existence of this warrant.

REQUEST FOR SEALING OF MATTER

57. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

LIMIT ON SCOPE OF SEARCH

58. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

59. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on computer systems owned, maintained, controlled and/or operated by TextNow, Inc., there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the electronic accounts described in Attachment A. The facts outlined above show that the TextNow, Inc. account, listed in Attachment A has been used for aggravated identity theft, money laundering, wire fraud mail fraud and conspiracy to commit these crimes in violation of 18 USC 1028A, 1956, 1343, 1341 and 371/1349, which items are more specifically described in Attachment B. There is probable cause to believe that the unidentified user of the Gmail account committed these offenses using the internet and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere. The account is the subject of this warrant affidavit. The account is: **619-720-0732**.

60. Law enforcement agents will serve the warrant on TextNow Inc., who will then compile the requested records at a time convenient to it, so there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

61. For these reasons, I request authority to seize all electronic communications and other content stored in the Target Account, to be searched off-site in a controlled environment. Law enforcement officers and agents will review the records sought by the search warrant and will segregate any messages and content constituting evidence, fruits or instrumentalities of violations of federal criminal law. Additionally, I request authority to serve the warrant on TextNow Inc. via the internet and to allow TextNow Inc. to copy the data outside of this agent's presence.


Dated: 12/23/20


Special Agent Jared R. Bahr
Department of Homeland Security
Investigations

Sworn to before me and:

- ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

this 23rd day of December, 2020


Daneta Wollmann
United States Magistrate Judge

ATTACHMENT A
Property to Be Searched

This warrant applies to the contents of and information associated with the following TextNow Inc. account, under an account known to be stored at the premises controlled by TextNow Inc., a company that accepts service of legal process at Attn: Registered Agent of Process for TextNow Inc., GKL Corporate/Search, Inc., Capitol Mall, Suite 660, Sacramento, CA 95814: **619-720-0732.**

ATTACHMENT B
**Particular Things to be Seized and Procedures
to Facilitate Execution of the Warrant**

**I. Information to be disclosed by TextNow Inc. (the “Provider”) to
facilitate execution of the warrant:**

To the extent that the information described in Attachment A is within the possession, custody, or control of TextNow Inc., including any emails, records, files, logs, or information that have been deleted but are still available to TextNow Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 23, 2020. TextNow Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A, including any information contained in the email account which is helpful to determine the accounts’ user’s or owner’s true identity:

a. The contents of all e-mails associated with the account, from the time of the account’s creation to the present, including stored or preserved copies of emails sent to and from the account, email attachments, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each e-mail;

b. The contents of all Instant Messages (IM) associated with the account, from the time of account’s creation to the present, including stored or preserved copies of IMs sent to and from the account, IM attachments, draft IMs, the source and destination addresses associated with each IM, the date and time at which each IM was sent, and the size and length of each IM;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP addresses used to register the account, all log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of services utilized;

e. All records or other information stored by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between TextNow Inc. and any person regarding the accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that was created or saved after the creation of the account that is the subject of this warrant and that constitutes contraband or fruits, evidence or instrumentalities of violations of 18 U.S.C. §§ 1028A, 1956, 1343, 1341 and 371/1349 (aggravated identity theft, money laundering, wire fraud mail fraud, and conspiracy, respectively), including, for the account or identifiers listed on Attachment A, information pertaining to the following matters:

- a. Any person communicating with others regarding stolen identifying information and that information being used to commit certain felonies, including fraudulent schemes, the laundering of illicit proceeds and the transfer of those proceeds, and the use of electronic communications and the U.S. Postal Service to facilitate these illegal acts;
- b. Any person sending images of identification documents, bank statements, other financial records, or any other records or description of records that may be used to facilitate the above offenses;
- d. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, or events relating to the crime under investigation and to the TextNow account owner(s) or user(s);
- e. Evidence indicating the TextNow account users or owner's state of mind as it relates to the crime under investigation;

- f. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- g. Records relating to who created, used, or communicated with the electronic account or identifier listed in Attachment A about matters relating to the criminal activity listed above, including identification of coconspirators, accomplices, and aiders and abettors in the commission of the above offenses, including records that help reveal their whereabouts.

2. Credit card information and money wire transmittal information, including bills, payment records, and any receipts, for payments to third party money remitters, including Xoom.com, Western Union, PayPal, and MoneyGram.

3. Evidence of who used, owned, or controlled the account or identifier listed on Attachment A, including evidence of their whereabouts;

4. Evidence of the times the user utilized the account or identifiers listed on Attachment A;

5. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifier listed on Attachment A and other associated accounts.

III. Information Regarding Search Warrant Compliance by TextNow:

TextNow shall disclose responsive data, if any, by sending to:

Special Agent Jared R. Bihr
Department of Homeland Security Investigations
1516 Fountain Plaza Drive
Rapid City, SD 57702
Jared.R.Bihr@ice.dhs.gov

TextNow shall use the United States Postal Service or another courier service to disclose the responsive data, notwithstanding 18 U.S.C. § 2252A or similar statute or code. In the alternative, TextNow may make the responsive data available to Special Agent Bihr by use of its law enforcement website.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL
RULE OF EVIDENCE 902(11) & (13)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by TextNow Inc., and my official title is _____.

I am a custodian of records for TextNow Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of TextNow Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of TextNow Inc.; and
- c. such records were made by TextNow Inc. as a regular practice.

I further state that this certification is intended to satisfy Rules 902(11) and (13) of the Federal Rules of Evidence.

Date

Signature

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of

USA v. 20-41-05

)
) Case No. 5:20-mj-248
)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 18 U.S.C. §§ 1028A, 1956, 1343, 1341, 371, 1349. See Affidavit in Support of Application for Search Warrant, and **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before January 6, 2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 12/23/20 at 9am,


Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

cc: AUSA Patterson - clr

Return		
Case No.: 5:20-mj-248	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized: 		
Certification		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	